Problem Sheet 4

11)

26^7

$(26^2)^3 \cdot 26$

$4 \cdot 26$

1) $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$

$1^2 \equiv 1 \bmod 5$

$2^1 \equiv 2 \bmod 5$
$2^2 \equiv 4 \bmod 5$
$2^3 \equiv 3 \bmod 5$
$2^4 \equiv 1 \bmod 5$

$3^1 \equiv 3 \bmod 5$
$3^2 \equiv 4 \bmod 5$
$3^3 \equiv 2 \bmod 5$
$3^4 \equiv 1 \bmod 5$

$4^1 \equiv 4 \bmod 5$
$4^2 \equiv 1 \bmod 5$

a	1	2	3	4	8
	1	4	4	2	

$\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

Scanned by CamScanner

b) $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$1^2 \equiv 1 \bmod 7$

$2^1 \equiv 2 \bmod 7$, $2^2 \equiv 4 \bmod 7$, $2^3 \equiv 1 \bmod 7$

$3^1 \equiv 3 \bmod 7$, $3^2 \equiv 2 \bmod 7$, $3^3 \equiv 6 \bmod 7$

$3^4 \equiv 4 \bmod 7$ $3^5 \equiv 5 \bmod 7$, $3^6 \equiv 1 \bmod 7$

$4^1 \equiv 4 \bmod 7$ $4^2 \equiv 2 \bmod 7$, $4^3 \equiv 1 \bmod 7$

$5^1 \equiv 5 \bmod 7$ $5^2 \equiv 4 \bmod 7$, $5^3 \equiv 6 \bmod 7$

$5^4 \equiv 2 \bmod 7$ $5^5 \equiv 3 \bmod 7$, $5^6 \equiv 1 \bmod 7$

$6^1 \equiv 6 \bmod 7$ $6^2 \equiv 1 \bmod 7$

a	1	2	3	4	5	6
ord(a)	1	3	6	3	6	2

$\mathbb{Z}_{13}^*$

a	1	2	3	4	5	6	7	8	9	10	11	12
ord(a)	1	12	3	6	4	12	12	4	3	6	12	2

2) $|\mathbb{Z}_5^*| = 4$ $|\mathbb{Z}_7^*| = 6$ $|\mathbb{Z}_{13}^*| = 12$

b) yes

5) $p = 467$ and $\alpha = 2$ $\phi(13) = 12$

a) $a = 3$ $b = 5$

Alice

$2^3 \bmod 467 = 8 = A$

$32^3 \bmod 467 =$

78

$\xrightarrow{A}$

$\xleftarrow[B]{}$

Bob

$B = 2^5 \bmod 467 = 32$

$K_{AB} = 8^5 \bmod 467$

$= 78$

b) $a = 400$ $b = 134$

Alice

$2^{400} \bmod 467$

$= 137$

$\xrightarrow{137}$

$\xleftarrow[84]{}$

$84^{400} \bmod 467$

$= 90$

Bob

$2^{134} \bmod$

$= 84$

$137^{134} \bmod$

$=$

$a = 22$

Alice

2^{228}

2) $\phi(4) = 2$ $\phi(7) = 6$ $\phi(13) = 12$

3) $p = 467$ and $\alpha = 2$

a) $a = 3$ $b = 5$

Alice

Bob

$2^3 \bmod 467 = 8 = A$

$B = 2^5 \bmod 467 = 32$

$$\xrightarrow{A}$$

$K_{AB} = 8^5 \bmod 467 = 78$

$$\xleftarrow[B]{}$$

$32^3 \bmod 467 = 78$

b) $a = 400$ $b = 134$

Alice

Bob

$2^{400} \bmod 467 = 137$

$2^{134} \bmod 467 = 84$

137

$a = 228$ $b = 57$

Alice

$2^{228} \bmod 467$

Bob

$2^{57} \bmod 467$

$\xrightarrow{394}$

$\xleftarrow{313}$

$394^{57} \bmod 467$
$= 206$

$313^{228} \bmod 467$
$= 206$

32

4) Both values would yield public keys that would immediately allow to recognise the private key.

If private key is 1, the public key would be α, if an attacker would detect this identity, he would know $K_{pr} = 1$

If $K_{pr} = p-1$, public key would take the value 1 according to FLT, an attacker could deduce $K_{pr} = p-1$

Scanned by CamScanner

5) Compute β : $\beta \equiv \alpha^d \bmod p$

Encrypt $(K_E, y) = (\alpha^i \bmod p, x\beta^i \bmod p)$

Decrypt $(K_E, y) = y(K_E^d)^{-1} \bmod p$

1) $(K_E, y) = (29, 296)$ $x = 33$

2) $(K_E, y) = (125, 301)$ $x = 33$

3) $(K_E, y) = (80, 174)$ $x = 248$

4) $(K_E, y) = (320, 139)$, $x = 248$

6) $y^2 \equiv x^3 + 2x + 2 \mod 17$

$$4a^3 + 27b^2 \not\equiv 0 \mod p$$

$$4(2)^3 + 27(2)^2$$

$$= 32 + 108 = 140$$

$$14 \not\equiv 0 \mod 17$$

b) $(\overset{x_1}{2}, \overset{y_1}{7}) + (\overset{x_2}{5}, \overset{y_2}{2})$

Point addition :-

$$s = \frac{y_2 - y_1}{x_2 - x_1} \mod p$$

$$= \frac{\cancel{7}\ 2-7}{5-2} \mod 17$$

$$= -5(3^{-1}) \mod 17$$

$$17 = 3(5) + 2$$

$$3 = 2(1) + 1$$

$$2 = 1(2) + 0$$

$$1 = 3 - 2$$

$$= 3 - (17 - 3(5))$$

$$= -17 + 6(3))$$

Inverse of 3 is 6

$S = -5(6) \bmod 17$

$S = 4$

$x_3 = 4^2 - 2 - 5 \bmod 17$

$= 9$

$y_3 = 4(2-5) - 7 \bmod 17$

$= 15$

$(9, 15)$

b) $(3, 6) + (3, 6)$

$$S = \frac{3(3^2) + 2}{2(6)}$$

$$= \frac{29}{12} \bmod 17$$

$= 29(12)^{-1} \bmod 17$

$12x \equiv 1 \mod 17$

$17 = 12(1) + 5$
$12 = 5(2) + 2$
$5 = 2(2) + 1$

$1 = 5 - 2(2)$
$= 5 - 2(12 - 5(2))$
$= 5(5) - 2(12)$
$= 5(17-12) - 2(12)$
$= 5(17) - 7(12)$

$a = -7 \quad a^{-1} = 10$

$s = 29(2) \mod 17 = 7$

$x_3 = 7^2 - 3 - 3 \mod 17 = 6$

$y_3 = 7(3 - 6) - 6 \mod 17 = 7$

$(6, 7)$

7) $17 + 1 - 2\sqrt{17} \approx 9$

$17 + 1 + 2\sqrt{17} \approx 26$

$9 \leq 19 \leq 26$

8)

8) $E: y^2 = x^3 + 3x + 2 \mod 7$

a) The points of E are
$\{(0,3), (0,4), (2,3), (2,4), (4,1), (4,6), (5,3), (5,4)\}$

b) Group order is $\#G = \cancel{\#}\ 9$

c) $0 \cdot \alpha = 0$
$1 \cdot \alpha = (0,3)$
$2 \cdot \alpha = (2,3)$
$3 \cdot \alpha = (5,4)$
$4 \cdot \alpha = (4,6)$
$5 \cdot \alpha = (4,1)$
$6 \cdot \alpha = (5,3)$
$7 \cdot \alpha = (2,4)$
$8 \cdot \alpha = (0,4)$
$9 \cdot \alpha = (0) = 0 \cdot \alpha$

$\mathrm{ord}(\alpha) = 9 = \#G$

α is primitive root

9) $E: y^2 \equiv x^3 + 4x + 20 \quad \mathbb{Z}_{29}$

a) $K = 9$

$9P = (1001)P$

Step 0:- Compute $P = 1P$

Step 1a:- Compute $P = 10P$ D $P + P = 2P$

Step 2a:- Compute $P = (100)P$ D $2P + 2P = 4P$

Step 3a:- Compute $P = (1000)P$ D $4P + 4P = 8P$

Step 3b:- Compute $P = (1001)P = 8P + P$ A

$= 9P$

$(4, 10) \leftarrow$ Final answer

b) $K = 20$

10100

$20P$:

Step 0:- Compute $P = 1P$

Step 1a:- Compute $P + P = 2P = 10 \cdot P$ D

Step 2a:- Compute $2P \cdot 2P = 4P = 100P$ D

Step 2b:- Compute $4P \cdot P = 5P = 101P$ A

Step 3a:- Compute $5P \cdot 5P = 10P = 1010$ D

Step 4a:- Compute $10P \cdot 10P = 20P = 10100P$

$P = (19, 13)$

10) $y^2 \equiv x^3 + x + 6 \mod 11$

Alice

Bob

$y^2 \equiv x^3 + x + 6 \mod 11$

A

$K_{pr} = 6$

Compute

$(5, 9)$

$K_{pub} = 6(\quad)$

K_{AB}

Compute $6(5, 9) = T_{AB}$

$6P = (110)P$

Step 0:- $P = 1P$

Step 1a:- $P = P + P = 2P = 10$ D

Step 1b:- $3P = 2P + P = 3P = 11$ A

Step 2a:- $6P = 3P + 3P = 6P = 110$ D

$K_{AB} = 2$

$P = (5, 9)$

$18x \equiv 1 \mod 11$

$(5, 9) + (5, 9)$

$$S = \frac{3x_1^2 + a}{2y_1} \mod 11$$

$$= \frac{3(5)^2 + 1}{2(9)} \mod 11$$

$$= 76 \cdot 18^{-1} \mod 11$$

$$= \cancel{76} \cdot 8 \mod 11 = 3 \mod 11$$

$$x_3 = S^2 - x_1 - x_2 \mod 11$$

$$= 3^2 - 5 - 5 \mod 11$$

$$= 10 \mod 11$$

$$y_3 = S(x_1 - x_3) - y_1 \mod 11$$

$$= 3(5 - 10) - 9 \mod 11$$

$$= 9 \mod 11$$

$(10, 9)$

$(5, 9) + (10, 9)$

$$S = \frac{9 - 9}{10 - 5} = 0$$

$x_3 = 0 - 10 - 5 \mod 11$
$= 7 \mod 11$

$y_3 = s(x_1 - x_3) - y_1 \mod 11$
$= -9 \mod 11$
$= 2$

$(7, 2)$

$(7, 2) + (7, 2)$

$s = \dfrac{3(7)^2 + 1}{2(2)} \mod 11$

$4x \equiv 1 \mod 11$

$= 5(4)^{-1} \mod 11$
$= 5(3) \mod 11$
$= 4$

$x_3 = s^2 - x_1 - x_2 \mod 11$
$= 4^2 - 7 - 7 \mod 11$
$= 2 \mod 11$

$y_3 = s(x_1 - x_3) - y_1 \mod 11$
$= \cancel{4 - 2 \mod 11} = 4(7 - 2) - 2 \mod$
$= 7$

$K_{AB} =$

5) Co
Enc
Dec

1)
2)
3)